(12) UK Patent Application (19) GB (11) 2 321 741 (13) A

(43) Date of A Publication 05.08.1998

(21) Application No 9702152.1

(22) Date of Filing 03.02.1997

(51) INT CL[6]
G07F 19/00 7/08

(52) UK CL (Edition P)
G4H HTG H1A H13D H14A

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition P) G4H HTG , H4P PDCSA
INT CL[6] G07F , H04L

(71) Applicant(s)
Certicom Corporation
(Incorporated in Canada - Ontario)
200 Matheson Boulevard, West, Suite 103,
Mississauga, Ontario L5R 3L7, Canada

(72) Inventor(s)
Scott A Vanstone

(74) Agent and/or Address for Service
Beresford & Co
2-5 Warwick Court, High Holborn, LONDON,
WC1R 5DJ, United Kingdom

(54) Abstract Title
Verification of electronic transactions

(57) In a method of verifying a pair of correspondents in an electronic transaction, the correspondents each include a first (e.g. RSA) and second (e.g. ECC) signature scheme. The first correspondent signs information according to the first signature scheme and transmits the first signature to the second correspondent which verifies it using the first signature scheme. The second correspondent signs information according to a second signature scheme and transmits the second signature to the first correspondent which verifies it using the second signature scheme. The transaction is rejected if either verification fails. The first and second correspondents may be a terminal 100 and smart card 102 respectively, and the invention permits the processing load on the card to be reduced.

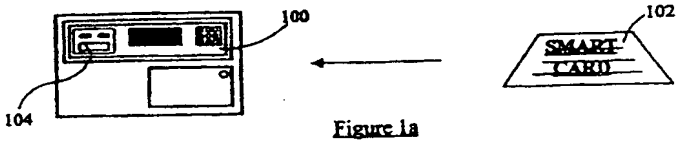

Figure 1a

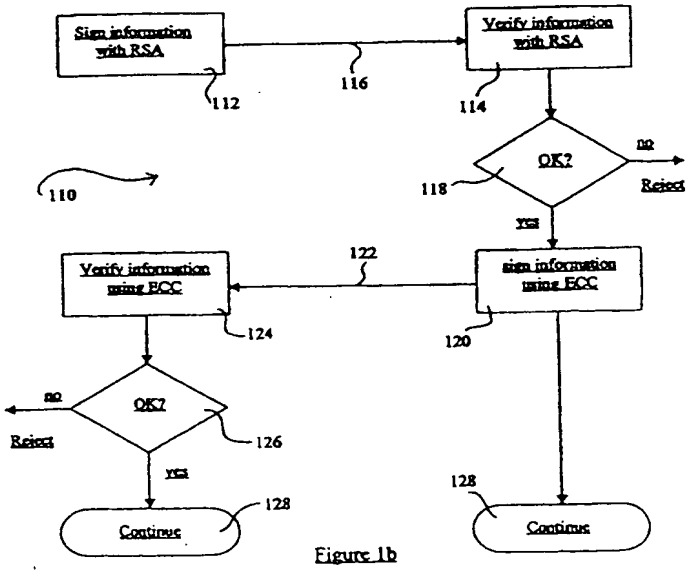

Figure 1b

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 321 741 A

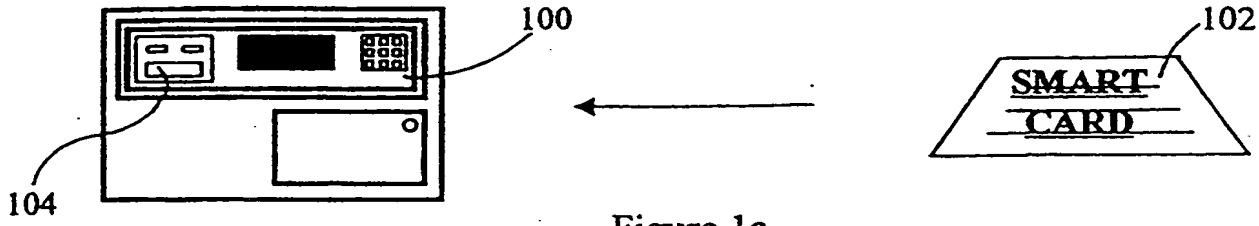

Figure 1a

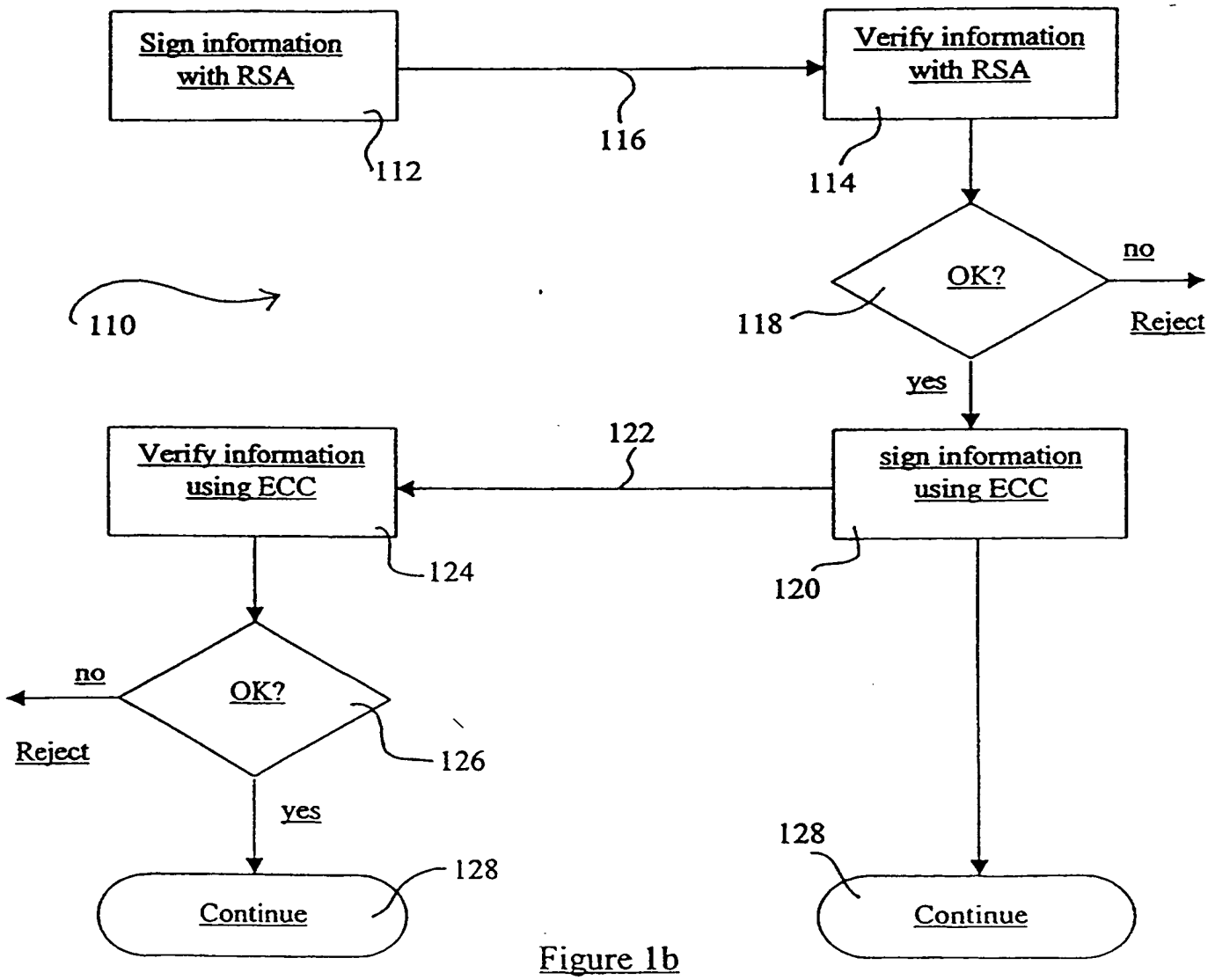

Figure 1b

DATA CARD VERIFICATION SYSTEM

This invention relates to methods and apparatus for data transfer and authentication in an electronic transaction system, and more particularly to electronic transaction systems utilizing smart cards.

BACKGROUND OF THE INVENTION

It has become widely accepted to conduct transactions such as financial transactions or exchange of documents electronically. Automated teller machines (ATMs) and credit cards are widely used for personal transaction and as their use expands so too does the need to verify such transactions increase. A smart card is somewhat like a credit card and includes some processing and storage capability. Smart cards are prone to fraudulent misuse, for example by a dummy terminal which is used to glean information from an unsuspecting user. Thus, before any exchange of critical information takes place between either a terminal and a smart card or vice versa it is necessary to verify the authenticity of the terminal as well as the card. One of these verifications may take the form of "signing" an initial transaction digitally so that the authenticity of the transaction can be verified by both parties involved in the subsequent session. The signature is performed according to a protocol that utilizes a random message, i.e. the transaction and a secret key associated with the party.

The signature must be performed such that the party's secret key cannot be determined. To avoid the complexity of distributing secret keys, it is convenient to utilize a public key encryption scheme in the generation of the signature. Such capabilities are available where the transaction is conducted between parties having access to relatively large computing resources, but it is equally important to facilitate such transactions at an individual level where more limited computing resources available, as in the smart card.

Transaction cards or smart cards are now available with limited computing capacity, but these are not sufficient to implement existing digital signature protocols in a commercially viable manner. As noted above, in order to generate a verification signature it is necessary to utilize a public key inscription scheme. Currently, most public

Furthermore, elliptic curve crypto-systems offer advantages over other key crypto-systems when bandwidth efficiency, reduced computation and minimized code space are application goals.

Furthermore, in the context of a smart card and an automated teller machine transaction, there are two major steps involved in the authentication of both parties. The first is the authentication of the terminal by the smart card and the second is the authentication of the smart card by the terminal. Generally, this authentication involves the verification of a certificate generated by the terminal and received by the smart card and the verification of a certificate signed by the smart card and verified by the terminal. Once the certificates have been positively verified the transaction between the smart card and the terminal may continue.

Given the limited processing capability of the smart card, verifications and signature processing performed on the smart card are generally limited to simple encryption algorithms. A more sophisticated encryption algorithm is generally beyond the scope of the processing capabilities contained within the smart card. Thus, there exist a need for a signature verification and generation method which may be implemented on a smart card and which is relatively secure.

SUMMARY OF THE INVENTION

This invention seeks in one aspect to provide a method of data verification between a smart card and a terminal.

In accordance with this aspect there is provided a method for verifying a pair of participants in an electronic transaction, comprising the steps of verifying information received by the second participant from the first participant, wherein the verification is performed according to a first encryption algorithm;

verifying information received by the first participant from the second participant, wherein the verification is performed according to a second encryption algorithm; and

whereby the transaction is rejected if either verification fails.

The first encryption algorithm may be one which is computationally more difficult in encryption than decryption, while the second encryption algorithm is more difficult in decryption than encryption. In such an embodiment the second participant may participate with relatively little computing power, while security is maintained at a high level.

Referring now to figure 2, a detailed implementation of the mutual authentication of the terminal and the card, according to the "challenged-response" protocol is shown generally by numeral 200. The terminal 100 is first verified by the card 102 and the card is then verified by the terminal. The terminal first sends to the card a certificate C_t, 20 containing its ID, T_{ID}, and public information including the public key. The certificate 20 may be also signed by a certifying authority (CA) so that the card may verify the association of the terminal ID T_{ID} with the public key received from the terminal. The keys used by the terminal and the CA in this embodiment may both be based on the RSA algorithm.

With the RSA algorithm each member or party has a public and a private key, and each key has two parts. The signature has the form:-

$$S = m^d \pmod n$$

where:

m is the message to be signed;

n a public key is the modulus and is the product of two primes p and q;

e the encryption key chosen at random and which is also public is a number chosen to be relatively prime to (p-1)x(q-1); and

d the private key which is congruent to $e^{-1} \pmod{(p-1)x(q-1)}$.

For the RSA algorithm, the pair of integers (n,e) are the public key information that is used for signing. While, the pair of integers (d,n) may be used to decrypt a message which has been encrypted with the public key information (n,e).

Referring back to figure 2, the numbers n and e are the public keys of the CA and may be set as system parameters. The public key e may be either stored in the smart card or in an alternate embodiment hardwired into an logic circuit in the card. Furthermore, by choosing e to be relatively small, ensures that the exponentiation may be carried out relatively quickly.

The certificate 20 C_t is signed by the CA and has the parameters (n,e). The certificate contains the terminal ID T_{Id}, and the terminal public key information T_n and T_e which is based on the RSA algorithm. The certificate C_t is verified 24 by the card extracting T_{ID}, T_n, T_e. This information is simply extracted by performing $C_t^e \bmod n$.

a is the long term private key of the sender(card) and has a corresponding public key aP = Q;

e is a secure hash, such as the SHA hash function, of a message m (R2 in this case) and short term public key R; and

n is the order of the curve.

For simplicity it will be assumed that the signature component s is of the form s = ae + k as discussed above although it will be understood that other signature protocols may be used.

To verify the signature sP-eQ must be computed and compared with R. The card generates R, using for example a field arithmetic processor (not shown). The card sends to the terminal a message including m, s, and R, indicated in block 44 of figure 2 and the signature is verified by the terminal by computing the value (sP-eQ) 46 which should correspond to kP. If the computed values correspond 48 then the signature is verified and hence the card is verified and the transaction may continue.

The terminal checks the certificate, then it checks the signature of the transaction data which contains R2, thus authenticating the card to the terminal. In the present embodiment the signature generated by the card is an elliptic curve signature, which is easier for the card to generate, but requires more computation by the terminal to verify.

As is seen from the above equation, the calculation of s is relatively straightforward and does not require significant computing power. However in order to perform the verification it is necessary to compute a number of point multiplications to obtain sP and eQ, each of which is computationally complex. Other protocols, such as the MQV protocols require similar computations when implemented over elliptic curves which may result in slow verification when the computing power is limited. However this is generally not the case for a terminal.

Although an embodiment of the invention has been described with reference to a specific protocol for the verification of the terminal and for the verification of the card, other protocols may also be used.

4. A method as defined in claim 1, said first digital signature scheme being a DSS type scheme and said second signature scheme being an elliptic curve type scheme.

5. A method of verifying a pair of correspondents in electronic transaction, said correspondents each including a first and second signature scheme, said method comprising the steps of:

said first correspondent transmitting to said second correspondent, a certificate including public key and identification information of said first correspondent;

said second correspondent verifying said certificate and extracting said public key and identification information therefrom;

said second correspondent generating a first challenge R_1 and transmitting said challenge to said first correspondent;

said first correspondent signing said received challenge R_1 in accordance with said first signature scheme;

said first correspondent generating a second challenge and transmitting said second challenge along with said signature C2 to said second correspondent;

said second correspondent verifying said signature C2 in accordance with said first signature scheme;

said second correspondent signing said second challenge R2 in accordance with said second signature scheme and transmitting said second signature to said first correspondent; and

said first correspondent verifying said second signature in accordance with said second signature scheme, whereby said transaction is rejected if either said first signature or said second signature is not verified.

6. A smart card for use in an electronic transaction, with a second correspondent, said card comprising:

a memory including

a first signature scheme consisting of a first signature generation algorithm and an associated verification algorithm;

a second signature scheme consisting of a second signature generation algorithm and an associated verification algorithm;

a program for invoking said algorithms; and

processor means for running said first verification algorithm for verifying first information received from said second correspondent and for running said second signature algorithm for signing a second information for transmission to said second correspondent.

7. A method of verifying a pair of correspondents substantially as hereinbefore described with reference to any of the accompanying drawings.

8. A smart card substantially as hereinbefore described with reference to and as illustrated in any of the accompanying drawings.

The Patent Office

Application No:	GB 9702152.1	**Examiner:**	Mike Davis
Claims searched:	1-8	**Date of search:**	26 March 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4H (HTG), H4P (PDCSA)

Int Cl (Ed.6): G07F, H04L

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
	None	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.